(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 December 2003 (31.12.2003)

PCT

(10) International Publication Number
WO 2004/002057 A3

(51) International Patent Classification[7]: H04L 9/06

(21) International Application Number:
PCT/IB2003/002623

(22) International Filing Date: 12 June 2003 (12.06.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
0214620.7 25 June 2002 (25.06.2002) GB

(71) Applicant *(for all designated States except US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HUBERT, Gerardus, T., M.** [NL/NL]; c/o Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(74) Agent: **TURNER, Richard, C.**; Philips Intellectual Property & Standards, Cross Oak Lane, Redhill, Surrey RH1 5HA (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

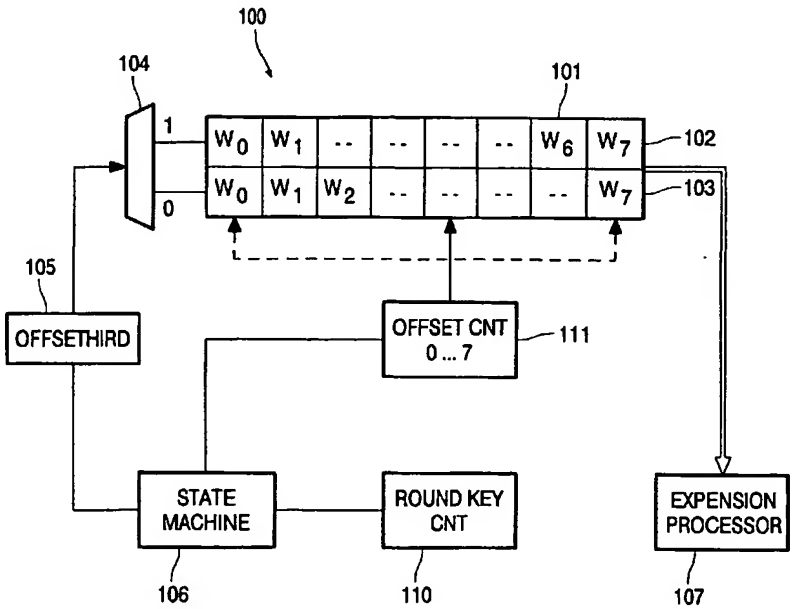
(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
21 May 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: ROUND KEY GENERATION FOR AES RIJNDAEL BLOCK CIPHER



(57) Abstract: Successive round keys of an expanded key according to the AES block cipher algorithm are generated from an initial cryptographic key, for use in a cryptographic (encryption and/or decryption) engine, in real time as the cryptographic process is executing. A limited key memory is used by overwriting previously generated words of the expanded key, leaving only the words of the initial key and the final key in the memory. Thus, a subsequent cryptographic operation can recommence either in the encryption or decryption direction, without delay to the cryptographic engine.

WO 2004/002057 A3

INTERNATIONAL SEARCH REPORT

Int[illegible]ional Application No
P[illegible]B 03/02623

A. CLASSIFICATION OF SUBJECT MA[illegible]
IPC 7 H04L9/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, INSPEC, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	DAEMEN J ET AL: "AES PROPOSAL: RIJNDAEL" AES PROPOSAL, XX, XX, PAGE(S) 1-45 , XP001060386 page 14, line 1 - page 15, last line - -/--	1-6,11, 12, 14-29, 34,35, 37-48

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
31 October 2003	16. 02. 2004
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Liebhardt, I

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int[redacted]jonal Application No
P[redacted]B 03/02623

C.(Continuation) DOCUMENTS CONSID[redacted]ED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	DAEMEN J ET AL: "Efficient block ciphers for smartcards" PROCEEDINGS OF THE USENIX WORKSHOP ON SMARTCARD TECHNOLOGY (SMARTCARD '99), PROCEEDINGS OF THE USENIX WORKSHOP ON SMARTCARD TECHNOLOGY, CHICAGO, IL, USA, 10-11 MAY 1999 , 1999, BERKELEY, CA, USA, USENIX ASSOC, USA, PAGE(S) 29 - 35 , XP002259943 ISBN: 1-880446-34-0 page 3, right-hand column, line 12 - line 37 page 6, left-hand column, line 1 - line 18	1-48
P,X	EP 1 292 066 A (AMPHION SEMICONDUCTOR LTD) 12 March 2003 (2003-03-12) paragraph '0007! paragraph '0043! - paragraph '0076! figures 9,9A,9B	1-6,11, 12, 14-29, 34,35, 37-48
P,X	EP 1 271 839 A (FUJITSU LTD) 2 January 2003 (2003-01-02) paragraph '0016! paragraph '0096! - paragraph '0122!	1-6,11, 12, 14-29, 34,35, 37-48

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/IB 03/02623

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☐ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

1-48

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☐ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-48

   Method and device for generating successive round keys of an expanded key for use in an encryption and/or decryption engine whereby previously generated words of the expanded key are cyclically overwritten so as to save memory.

   ---

2. claims: 49-54

   AES round constant function generator comprising a register and control inputs for controling the shifting of the register contents.

INTERNATIONAL SEARCH REPORT

International Application No
P[redacted]B 03/02623

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 1292066 A	12-03-2003	EP 1292066 A1	12-03-2003
		US 2003059054 A1	27-03-2003
EP 1271839 A	02-01-2003	JP 2003015522 A	17-01-2003
		EP 1271839 A2	02-01-2003
		US 2003108195 A1	12-06-2003